

Confidential

NOV 08 2018

JAMES N. HATTEN, Clerk
[Signature] Deputy Clerk

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

COMMON CAUSE GEORGIA,
as an organization,

Plaintiff,

v.

BRIAN KEMP, in his official
capacity as Secretary of State of
Georgia,

Defendant.

CIVIL ACTION FILE

NO. 1:18-CV-05102-~~ELR~~ *AT*

DECLARATION OF THERESA PAYTON

Pursuant to 28 U.S.C. § 1746, THERESA PAYTON, Chief Executive Officer of Fortalice Solutions, declares as follows:

I make this Declaration in support of a response by Secretary of State Brian Kemp to the motion for a temporary restraining in the above-styled matter of *Common Cause Georgia, v. Brian Kemp* (Civil Action No. 1:18-cv-05102-ELR).

1.

I am the Chief Executive Officer of Fortalice Solutions. Fortalice Solutions is a full service cyber-security company that offers businesses and

JMP 11/8/18

governments a full suite of cyber-security services, including cyber-security assessments, vendor assessments, penetration testing, review of cyber-security policies and procedures, and cyber incident response and analysis.

2.

Prior to co-founding Fortalice, I was Chief Information Officer for The Office of Administration, Executive Office of the President at the White House from 2006-2008, overseeing all information technology and information security functions. I am the co-author of numerous books and articles regarding cyber-security, including *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights*, and *Protecting Your Family and Protecting Your Internet Identity: Are You Naked Online?* I was named one of the 25 Most Influential People in Security by Security Magazine. My curriculum vitae is attached as Exhibit A to this declaration.

3.

The Georgia Secretary of State's Office ("SOS") has been a Fortalice client since Spring 2016. Fortalice has provided cyber-security assessments of SOS networks, including elections related networks. We have also conducted penetration testing of these networks, reviewed cyber-security policies and procedures, and from time to time, conduct cyber-incident response and analysis. Our incident response and analysis activities involve reviewing log

JMP 11/8/18

files from certain servers and applications to determine what activity has occurred and whether any attempts to penetrate systems have been successful, attempt to isolate malicious activity, and attempt to determine where any malicious activity originates.

4.

SOS engaged Fortalice to review a threat that it received regarding an attempted infiltration of the My Voter Page (MVP) system. My team reviewed the file that outlines the alleged vulnerabilities, tested the alleged vulnerabilities with express permission from SOS, and reviewed system logs to determine if any vulnerability had been successfully exploited. Thus far, our incident response team has reviewed logs dating back two weeks from the date of the alleged incident, and a more thorough review is in progress. It is common to see servers that are internet-facing have attempted attacks launched against them and similar in nature to the alleged attack.

5.

In reviewing the logs of the MVP system, Fortalice has seen multiple unsuccessful attempts to infiltrate that system. To date, in our analysis, we have not seen any successful attempts. More analysis work is underway and we continue to review logs to gather internet protocol and other identifying information to help determine the source of these attempts.

JMP 11/8/18

6.

My team has also carried out a preliminary review of the SOS provided logs from the last two weeks that monitor the traffic into and out of the ENET server, which is a completely separate system from MVP housed on a completely separate server. The security posture of the ENET server is very different than the posture of the MVP server, as would be expected based on my understanding of the different purposes of those applications. The logs from the ENET network monitor do not show any malicious or unusual activity.

We are in the process of carrying out a forensic review of the system to determine if there was any unusual activity on the device

I declare under penalty of perjury that the foregoing is true and correct to the best of my ability.

Executed this 8th day of November, 2018.

A handwritten signature in black ink, appearing to read 'Theresa Payton', is written over a horizontal line.

THERESA PAYTON
Chief Executive Officer
Fortalice Solutions LLC